Burgan Bank

Artificial Intelligence Policy

بنک برقان
BURGAN BANK

Introduction

This Policy has been developed by and is exclusive property of Burgan Bank. The Policy is publicly intended solely for informational purposes. No part of this Policy may be copied, reproduced, distributed, modified, or transmitted in any forms or any means without the prior written consent of Burgan Bank. Any unauthorized use, reproduction, distribution, or modification of this Policy may result in legal action in accordance with applicable laws and regulations.

Introduction

This Policy sets out Burgan Bank's commitments and requirements for responsible AI governance and use. The AI Governance Framework supports implementation of its principles, objectives and requirements.

Policy Statement

Burgan Bank (the Bank) intends to implement an Artificial Intelligence Management System (AIMS) aligned with the Central Bank of Kuwait (CBK) Cyber and Operational Resilience Framework (CORF) and leading industry standards, including ISO/IEC 42001 and the NIST AI Risk Management Framework, to support secure and trusted AI practices.

The Policy defines authority and control over AI systems, models, assets and associated infrastructure, and how they may be used. It encompasses the people, processes and technologies required to manage and protect AI systems.

The Bank's AI Policy establishes a security-focused approach to AI adoption and use, supported by governance controls, systematic risk assessment, security by design, testing, human oversight and the authority to suspend or shut down AI systems when risks arise.

Purpose

- Establish AI governance principles, accountability and responsibilities.
- Harmonize AI development, deployment, outsourcing and use within the Bank.
- Balance business needs and security measures and support AI-driven business decisions.
- Promote transparency, explainability, ethical use and meaningful human oversight.
- Identify, assess, mitigate and monitor AI-specific risks in alignment with the Bank's risk appetite.
- Protect AI systems and the quality, integrity and privacy of the data they use.
- Promote awareness of responsible AI use and comply with applicable legal, regulatory and contractual obligations.

Scope

This Policy applies to Bank employees and third-party personnel, including contractors and service providers, who access or act on behalf of the Bank in relation to its AI systems. It covers AI technologies under the Bank's control, whether developed in-house, purchased from vendors or integrated within larger software platforms.

The scope includes machine learning, deep learning, language models, generative AI, agentic AI, AI agents, retrieval-augmented generation and other AI technologies and methodologies.

Responsibilities

The Board of Directors and Senior Management shall establish an enabling structure for effective AI management and adherence to sound operating procedures. AI governance responsibilities shall be defined across strategic, managerial and operational levels.

Board of Directors

- Approve the AI Policy, review it annually and authorize changes.
- Make high-level AI management decisions and resolve unresolved conflicts.
- Review serious ethical concerns relating to AI use and outputs.
- Establish AI-specific risk tolerance levels and allocate resources for AI management.

AI Governance and Management

The Bank's AI governance arrangements shall provide cross-functional direction and oversight, support implementation of the AI Governance Framework, allocate responsibilities and promote continual improvement. Relevant departments shall support AI governance coordination and lifecycle oversight in accordance with the Bank's internal responsibility assignments.

IT, business and relevant governance functions shall support strategic alignment, escalation of critical AI governance issues, ethical AI practices, communication, awareness and implementation in accordance with the Bank's internal governance arrangements.

Information and Cyber Security Department (ICSD)

ICSD participates in the Bank's cross-functional AI governance arrangements and is consulted in the execution of the AI Policy.

Employees and Third Parties

Compliance with the AI Policy is mandatory for employees, associates, contractors and third parties, as applicable. Individuals using AI tools remain accountable for their tool-based decisions and for AI systems entrusted to them. Failure to comply may result in disciplinary action.

Human Oversight and Accountability

AI shall support human decision-making, expertise and creativity in service of the Bank's business objectives. Meaningful human oversight and intervention shall be preserved, particularly in critical applications.

AI-generated decisions shall be logged to support traceability. Responsibilities for investigating, escalating and resolving AI errors and failures shall be assigned, and oversight and redress mechanisms shall support accountability for lawful, ethical and responsible operation.

AI Suspension and Shutdown Safeguard ("Kill Switch")

The Bank's AI governance arrangements shall provide for a deactivation mechanism ("kill switch") for all AI systems deployed within the Bank. In the event of malfunction, unintended behavior or risk arising from AI operations, immediate suspension or shutdown may be initiated to mitigate potential harm or adverse impact. Ownership and exclusive activation authority shall remain as assigned under the Bank's internal AI Policy.

Principles of AI Governance

The following principles guide the Bank's AI management and governance:

Accountability and Responsibility: Individuals using AI tools remain accountable for their tool-based decisions and responsible and ethical AI use.

Risk-Aware Culture: AI risks shall be recognized and managed throughout the AI lifecycle, with responsibilities embedded within the Bank's organizational culture.

Supply Chain Due Diligence: Prospective third parties and relevant sub-providers shall be assessed before entering, amending or renewing AI arrangements.

Compliance: AI initiatives shall adhere to applicable laws, regulations and industry standards, supported by ongoing compliance monitoring.

Security by Design: AI systems and data shall be protected through security measures, testing and regular audits.

Transparency and Trust: AI use and governance processes shall be communicated clearly to internal and external stakeholders.

Ethical AI Development, Deployment and Use: AI shall be designed, developed and used to minimize bias, uphold fairness and non-discrimination, and support ethical outcomes.

Responsible Data Governance: Data quality, integrity and privacy shall be maintained through governance practices supporting responsible AI use.

Technology and Algorithm Neutrality: The Policy applies across AI technologies, algorithms and methodologies, regardless of development language or data storage methods.

In Service of Business: AI shall enhance human decision-making, expertise and creativity in alignment with the Bank's mission, vision and business model.

Continuous Improvement and Innovation: AI practices shall evolve with technological advancements, lessons learned and emerging best practices.

AI Security, Guardrails and Risk Management

The Bank shall systematically identify, assess, mitigate and monitor AI-specific risks in alignment with its established risk appetite and AI risk management methodology. AI governance shall be integrated with enterprise risk management and audit frameworks.

AI Governance Framework

The Burgan Bank AI Governance Framework (AIGF) serves as the primary operational document for implementing the AI Policy. The Policy requires AI governance controls to form part of the Bank's cybersecurity framework and AI governance processes to be integrated with enterprise risk management and audit frameworks.

Security Measures and Governance Guardrails

The Bank's AI Policy and its relevant governance documents provide safeguards for responsible AI use through security by design, validation before deployment, documented limitations and boundaries, meaningful human oversight, decision traceability and prohibited-use restrictions. These safeguards establish governance guardrails for responsible AI development, deployment and use.

AI systems and data are protected against threats and vulnerabilities through robust security measures, thorough testing and regular audits. Scenario testing and simulations shall validate AI reliability and ethical outcomes.

Risk Assessment and Monitoring

- Maintain an inventory of AI models and systems and update relevant asset records as new AI systems or models are introduced.
- Apply security measures and data governance practices to AI systems developed, deployed or outsourced by the Bank.
- Validate intended uses, beneficial outcomes, limitations and stakeholder expectations before deployment.
- Conduct scenario testing and simulations to validate AI reliability and ethical outcomes.
- Monitor AI system effectiveness and compliance and refine and improve AI management practices.

Third-Party AI Systems

The Bank shall conduct due diligence on prospective third parties and relevant sub-providers before entering, amending or renewing AI arrangements. Internal governance and IT security requirements shall apply to third-party AI systems, data and software, whether open source, commercial or proprietary.

Third-party vendors and partners shall adhere to the Bank's AI governance standards. Outsourced AI systems remain subject to the Bank's requirements for security, data quality, integrity, privacy and responsible use.

Training and Awareness

The Bank shall provide training and awareness on AI management and acceptable AI use. Relevant governance functions shall support comprehensive training across applicable Bank functions and promote ethical awareness and a risk-aware culture.

Compliance and Review

The Bank's AI Policy requires prior CBK approval before adopting any new AI model, system or use case. The approval request shall include risk assessment outcomes and risk mitigation measures, together with details of the technology and its application. AI initiatives shall

comply with applicable laws, regulations, internal policies and contractual obligations. The AI Policy shall be reviewed annually and when significant changes, evolving business requirements or relevant management decisions affect it. Compliance shall be assessed through periodic reviews and audits, with findings documented and reported to the Board of Directors.

Permitted deviations shall require written authorization and documented risk assessment under the Bank's internal governance arrangements. The prohibited uses below do not permit exemptions.

Prohibited AI Uses

The following uses of AI are prohibited under the Bank's AI Policy, with no exemptions permitted:

- Sharing proprietary information about Bank projects or products with external AI systems, including information classified as Restricted or Confidential, trade secrets or information otherwise protected by law.
- Using AI for unlawful activities, including threats, intimidation, harassment, defamation or the promotion of violence, terrorism or illicit goods and services.
- Deploying or using Shadow AI within the Bank.
- Using AI to circumvent user authentication, bypass security measures, or interfere with or disable Bank systems.
- Creating or disseminating defamatory, libelous or reputation-damaging AI content, including false or misleading information, through Bank or external AI systems.
- Using AI to create, modify, store or transmit discriminatory, misleading, harmful or offensive outputs, or outputs inconsistent with the Bank's ethical, regulatory or professional standards.
- Using AI to identify or classify employees, contractors, clients or other affiliated stakeholders based on personally identifiable information, including HR screening of applicants based on such characteristics.
- Using AI to generate or provide legal advice, including drafting, reviewing or approving internal policies, contracts or documents intended for distribution to third parties. Legal matters shall be referred to qualified legal professionals under established procedures.

Abbreviations

Term	Meaning
AI	Artificial Intelligence
AIGF	Burgan Bank AI Governance Framework
AIMS	Artificial Intelligence Management System
CBK	Central Bank of Kuwait
CORF	Cyber and Operational Resilience Framework
AI System	AI models, data processes, interfaces and supporting technology used to perform a task
External AI System	AI Technology or services developed, hosted or operated by third parties outside the Bank.
Approved AI Tools	AI systems officially authorized for use within the Bank under its security, privacy, risk and governance controls.
ICSD	Information and Cyber Security Department
the Bank	Burgan Bank
Shadow AI	AI tools or software used within the Bank without formal approval or oversight.